protiviti®
Face the Future with Confidence

MAKING CENTS OF RISK:

CASE STUDIES AND TOOLS TO COMMUNICATE THE REAL DOLLAR COSTS OF RISK

March 2021

Internal Audit, Risk, Business & Technology Consulting

TODAY'S TOPICS

Data Privacy: the gift that keeps on giving

Winter is Coming: enforcement and fines

Risk Quantification: the classic matrix model

Risk Quantification: upgrading to FAIR

POLL QUESTION #1

GLOBAL DATA PRIVACY: THE GIFT THAT KEEPS ON GIVING

WHAT IS PRIVACY?

What is the difference between security and privacy?

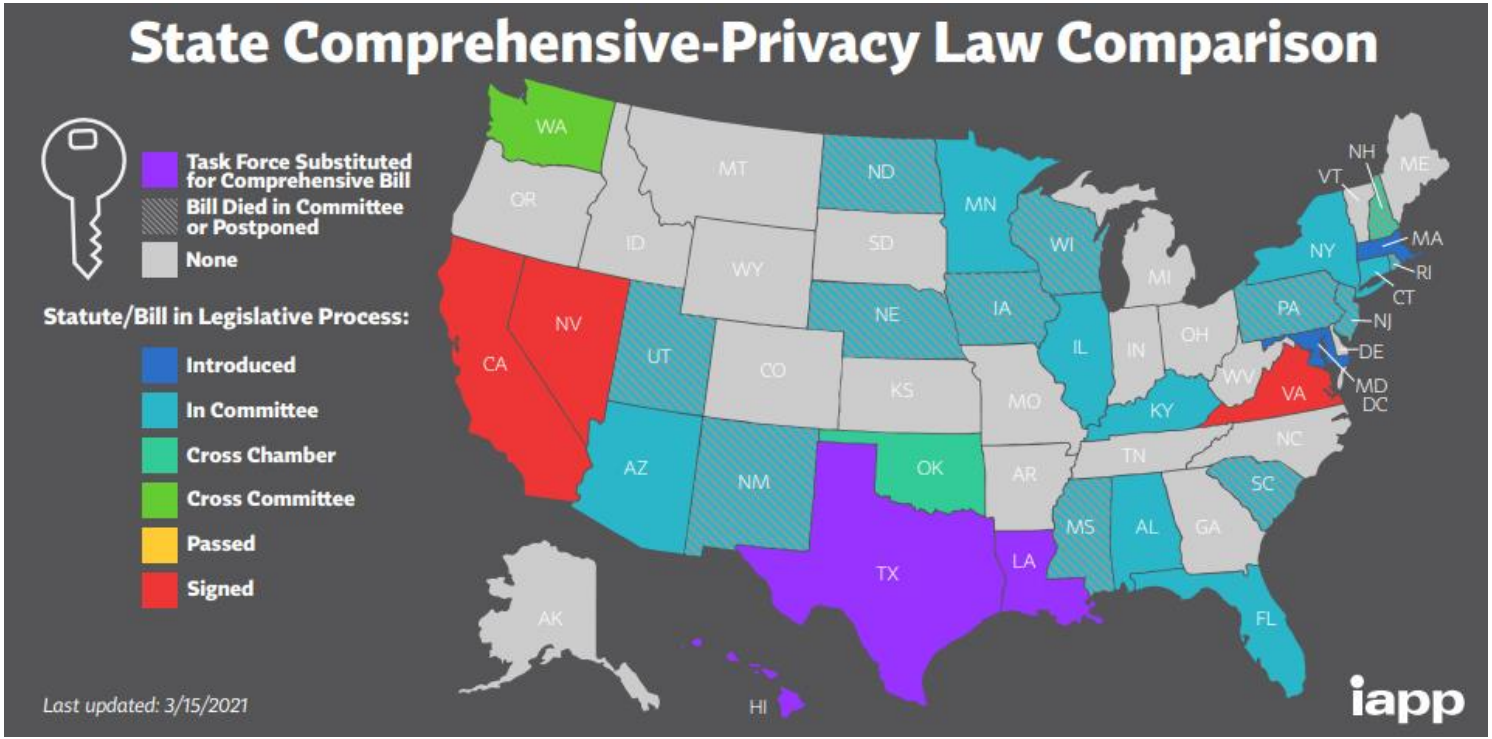
*Privacy relates to any **rights** you have to control **your personal information*** and how it's used.

Security, on the other hand, refers to ***how your personal information is protected***

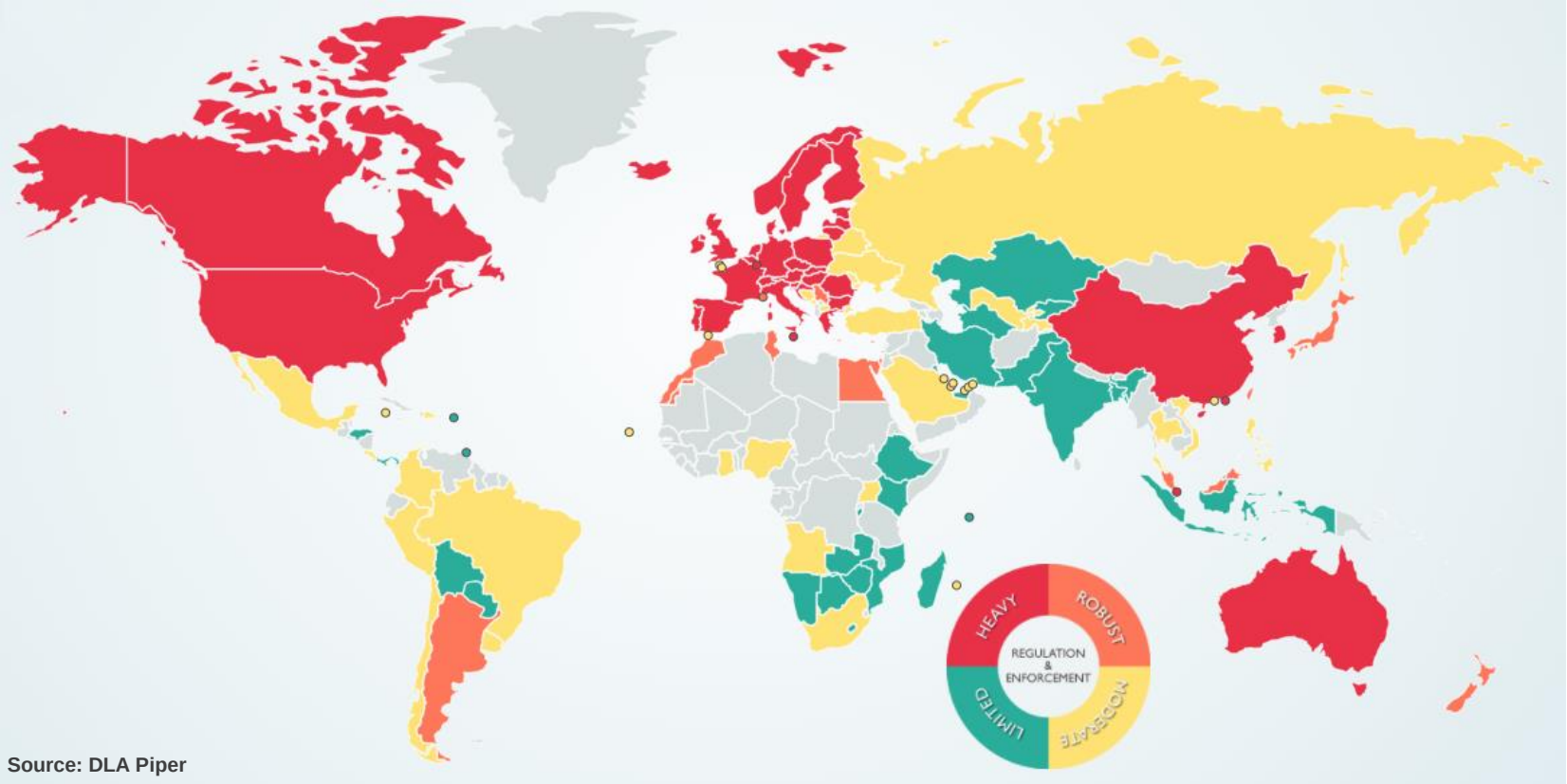
US PRIVACY LANDSCAPE

ARE YOU IN FAVOR OF FEDERAL PRIVACY LEGISLATION?

California has paved the way for change across the U.S. privacy landscape with many states following suit by introducing draft Bills, some of which exceed the CCPA in scope.



INTERNATIONAL DATA PRIVACY OUTLOOK



Source: DLA Piper

ENFORCEMENT & FINES

FINES AND MORE FINES

Google hit with largest GDPR fine to date over lack of data and ad transparency

"As a result, Google was fined €50 million and could receive further penalties if it does not amend these practices. To date, this is the largest fine…"

19 Jan 2019 – 9to5google.com

Germany fines H & M 35 million euros for data protection breaches

"Sweden's H&M has been fined 35 million euros ($41 million) by the German authorities for internal data security breaches at its customer service centre in Nuremberg."

20 Oct 2020 – reuters.com

Italian Telecommunications Operator TIM - $31.5 million USD

"The Italian Data Protection Authority…most of which stem from an overly-aggressive marketing strategy. Millions of individuals were bombarded with promotional calls and unsolicited communications, some of whom were on non-contact and exclusion lists."

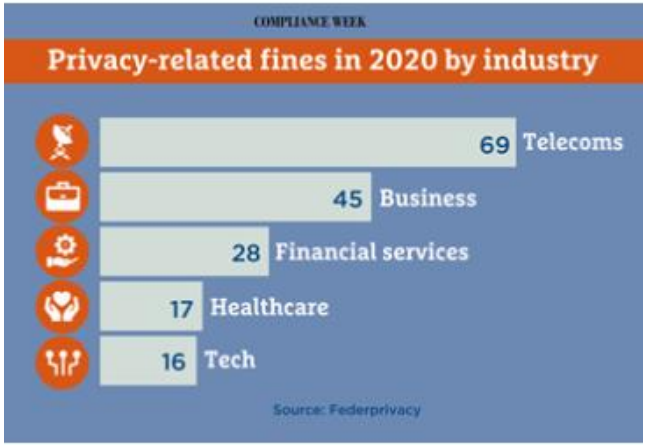
23 Nov 2020 – complianceweek.com

WHAT CAN WE LEARN FROM GDPR?

From Jan 2020 – Jan 2021:

- GDPR fines rose by nearly **40%**
- Penalties under the GDPR totaled €158.5 million ($**191.5 million**) last year alone. Approximately $332.4 million to date.
- Data protection authorities recorded **121,165** data breach notifications (**19% more** than the previous 12-month period)

Source: DLA Piper Research



A Schrems-II related violation may have material adverse impacts on your organization (up to 4% of annual global turnover) and exposes the Board of Directors to personal liability for failure to act, making this a relevant topic for the Board of Directors, Shareholders & External Auditors.

WHAT IS THE INEVITABLE FUTURE?

Prepare for NY Data Privacy Law to Catch Up to Calif.

"Governor Andrew M. Cuomo today announced a comprehensive law that will provide New Yorkers with transparency and control over their personal data and provide new privacy protections as part of the 2021 State of the State."

15 January 2021 – governor.ny.gov

CALIFORNIA PRIVACY RIGHTS ACT IMPACT ON BUSINESS

"The California Privacy Rights Act (CPRA) amend the California Consumer Privacy Act (CCPA). While most of the provisions in the CPRA do not go into effect until Jan 1, 2023, the changes do cover personal information collected as of Jan. 1, 2022

28 Jan, 2021 – The National Law Review

Virginia Consumer Data Protection Act: Here comes the Next State Privacy Law of the Land

On March 2, 2021, Virginia Governor Ralph Northam signed the Consumer Data Protection Act (CDPA or law) into law. This makes Virginia the second state, behind California, to adopt a comprehensive consumer data privacy law.

8 March 2021 – JD Supra

DATA SUBJECT / CONSUMER RIGHTS

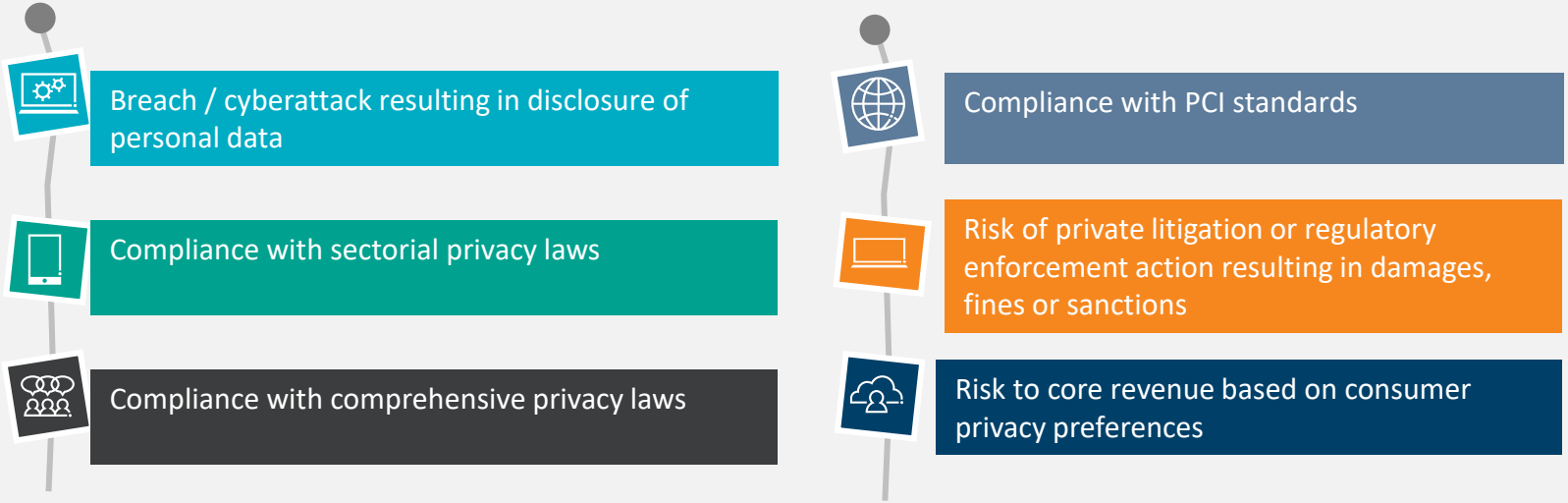
Individual Right	GDPR	CCPA	CPRA
Right to be **Informed**	Right to be given information about how personal data is being processed and why	Right to be given information about the categories of personal data that is being collected, prior to collection taking place and upon request	Right to request access to and knowledge about *decision making* technologies and probable outcomes
Right to **Access**	Right to access all personal data in a user-friendly, readable format.	Right to access personal data collected in the last 12 months, delineated between sold and transferred	-
Right to **Portability**	Must export personal data processed in a machine-readable file format.	Must export personal data collected in the last 12 months in a machine-readable file format	-
Right to **Correction**	Right to correct personal data	-	Right to correct PI and sensitive PI if found to be inaccurate
Right to **Stop or Limit Processing**	Right to withdraw consent and stop processing personal data	Right to opt-out of selling personal data only; but there is no requirements to stop collection/processing	Right to restrict use of PI, particularly around third-party sharing
Right to **Stop Automated Decision-Making**	Right to require a human to make decisions that have a legal effect	-	Right to opt-out of data being used to make automated inference (e.g. target profiling, behavioral advertisement)
Right to **Erasure**	Right to erase personal data processed, under certain conditions	Right to erase personal data collected, under certain conditions	-
Right to **Equal Services & Price**	Implicitly required	Explicitly required	-
Private **Right of Action Damages**	No limitation of liability	Liability is limited from $100 to $750 per individual per incident	-
Regulator Penalties	***Limited to 20 million or 4% of global revenue (whichever is greater)***	***No limitation - $7,500 per individual violation***	***Extends the scope of the private right of action by adding a cause of action***

NOTE: The new Virginia Consumer Data Protection Act passed in March 2021 and adds a new right: the Right to Opt-Out of Targeted Advertising. This law takes effect January 1, 2023.

POLL QUESTION #2

THE RESULTS ARE IN – 2020 PRIVACY RISK STUDY

Targeted industry sectors include: B2C & B2B technology, pharmaceutical & health services, banking & finance, retail, and insurance.



Source: IAPP – Privacy Risk Study 2020

RISK QUANTIFICATION: THE CLASSIC MATRIX MODEL

POLL QUESTION #3

CYBER RISK MATURITY CONTINUUM

Fear, Uncertainty & Doubt → Compliance Checklists → Maturity Models → Operational Performance → Cyber Risk Economics

Are we spending our cybersecurity budget on the right things? What is the ROI?

How much risk do we have? Are we spending too much or too little?

Do we have enough cyber insurance?

We don't want to be the next news headline cybercrime victims. Are we doing enough to minimize risk?

Board, CFO, ERM, CIO

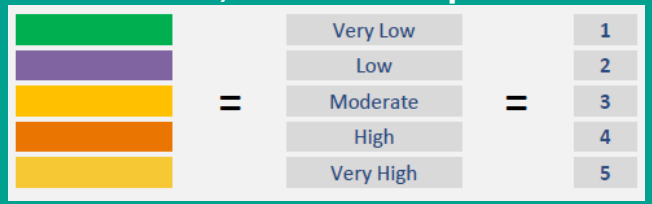
COMPLIANCE ≠ RISK

Qualitative Checklists & Frameworks

NIST

ISO 27001 Certified

Governance, Risk & Compliance Tools



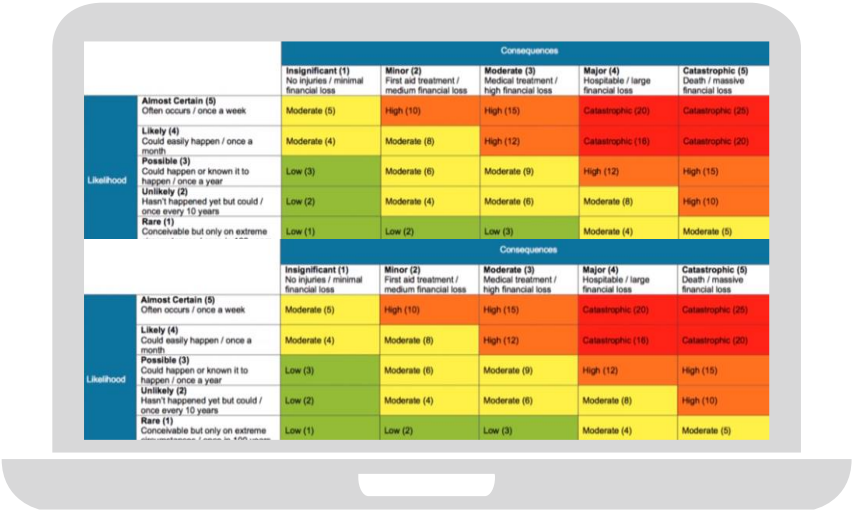
The way most organizations measure risk today fails to quantify information and operational risk in terms that the business can understand and use.

Robert Half protiviti

“PSEUDO-QUANTITATIVE” METHODS

Using Risk Matrices, assigning risk scores or ratings, and other “pseudo-quantitative” methods to assess risk creates 3 main problems.

- **Fake Math**
- **Inability to Aggregate Risk**
- **Inability to Communicate Risk**



Just because you’ve assigned numbers to risks doesn’t mean you can do math with those numbers!

FAKE MATH

		Consequences				
		Insignificant (1) No injuries/ minimal financial loss	**Minor (2)** First aid treatment/ medium financial loss	**Moderate (3)** Medical treatment/ high financial loss	**Major (4)** Hospitable/ large financial loss	**Catastrophic (5)** Death / massive financial loss
Likelihood	**Almost Certain (5)** Often occurs/ once a week	Moderate (5)	High (10)	High (15)	Catastrophic (20)	Catastrophic (25)
	Likely (4) Could easily happen/ once a month	Moderate (4)	Moderate (8)	High (12)	Catastrophic (16)	Catastrophic (20)
	Possible (3) Could happen or known it to happen/ once a year	Low (3)	Moderate (6)	Moderate (9)	High (12)	High (15)
	Unlikely (2) Hasn't happened yet but could/ once every 10 years	Low (2)	Moderate (4)	Moderate (6)	Moderate (8)	High (10)
	Rare (1) Conceivable but only on extreme circumstances/ once in 100 years	Low (1)	Low (2)	Low (3)	Moderate (4)	Moderate (5)

FAKE MATH – IT DOESN'T ADD UP

>40%	Likely	6	6	12	18	24	30	36	Risk Score	Rank
20%<p<=40%	Occasional	5	5	10	15	A 20	25	30	A=20	1
10%<p<=20%	Seldom	4	4	8	12	16	20	24	B=15	2
5%<p<=10%	Unlikely	3	3	6	9	12	B 15	18	C=12	3
1%<p<=5%	Remote	2	2	4	6	8	10	C 12		
<=1%	Rare	1	1	2	3	4	5	6		
			1	2	3	4	5	6		
			Incidental	Minor	Moderate	Major	Severe	Catastrophic		
			<=$100k	$100-250k	$250k-1M	$1-5M	$5-20M	>$20M		

RANKING IS COMPLETELY ARBITRARY

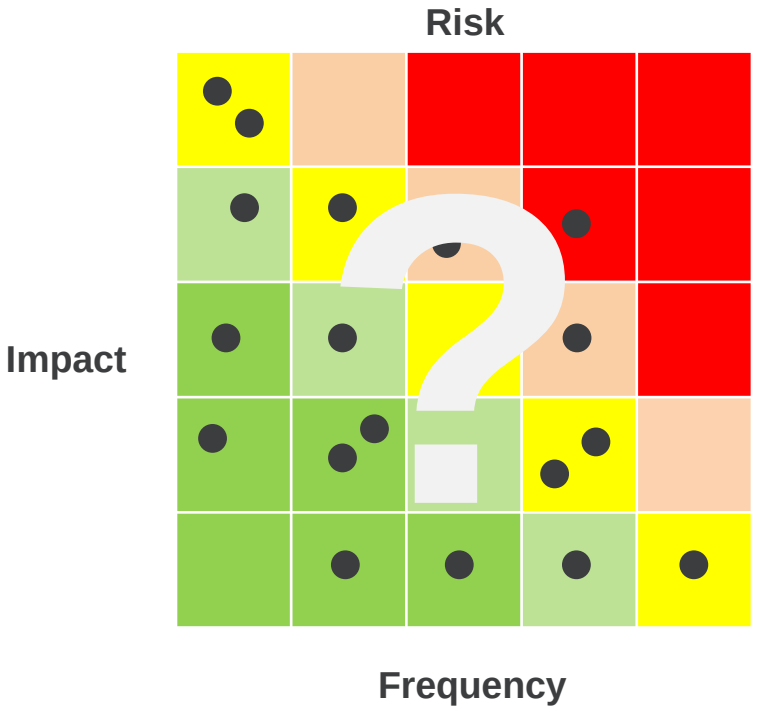
>40%	Likely	1	6	5	4	3	2	1	Risk Score	Rank
20%<p<=40%	Occasional	2	12	10	8	A 6	4	2	A=6	2
10%<p<=20%	Seldom	3	18	15	12	9	6	3	B=8	1
5%<p<=10%	Unlikely	4	24	20	16	12	B 8	4	C=5	3
1%<p<=5%	Remote	5	30	25	20	15	10	C 5		
<=1%	Rare	6	36	30	24	18	12	6		
			6	5	4	3	2	1		
			Incidental	Minor	Moderate	Major	Severe	Catastrophic		
			<=$100k	$100-250k	$250k-1M	$1-5M	$5-20M	>$20M		

Reference: Thomas, Philip & Bratvold, Reidar & Bickel, J. (2013). The Risk of Using Risk Matrices

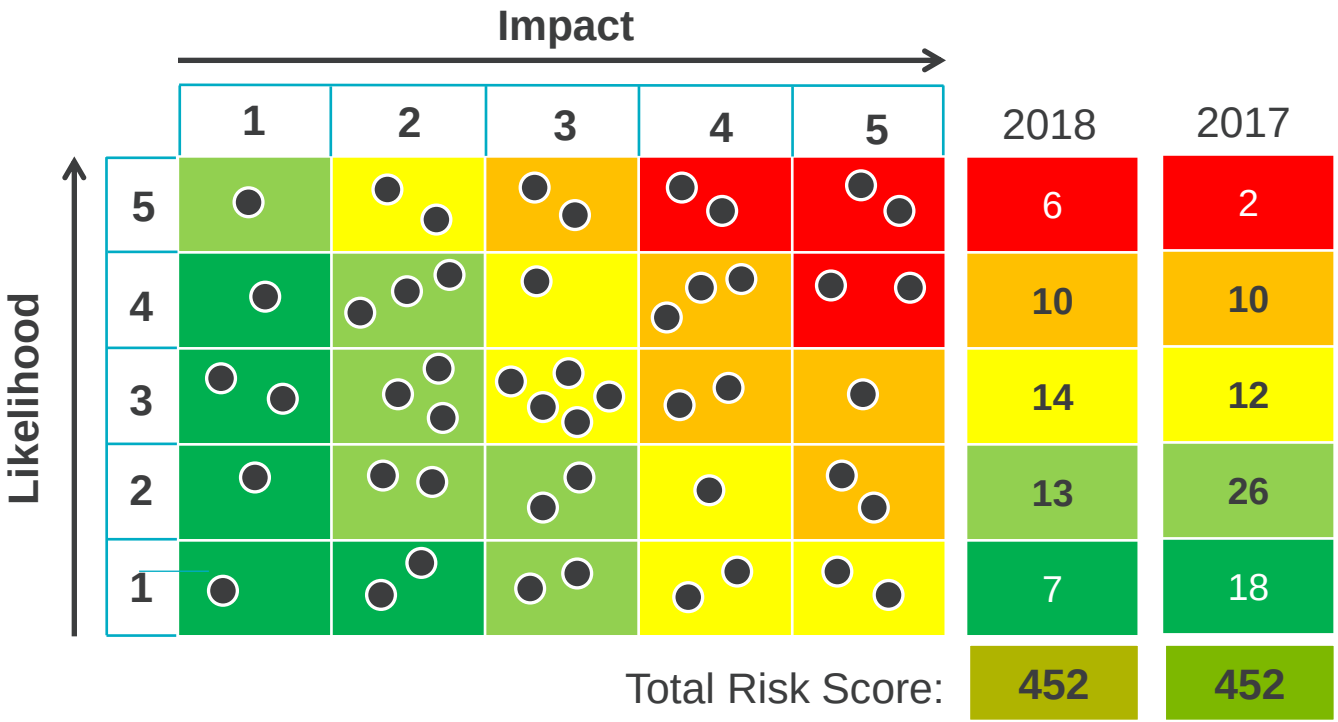
RISK AGGREGATION

How much risk is the business facing?

- This year?
- In a business unit?
- To a specific asset?



RISK AGGREGATION – LOST IN THE MIX



POLL QUESTION #4

SUBJECTIVITY

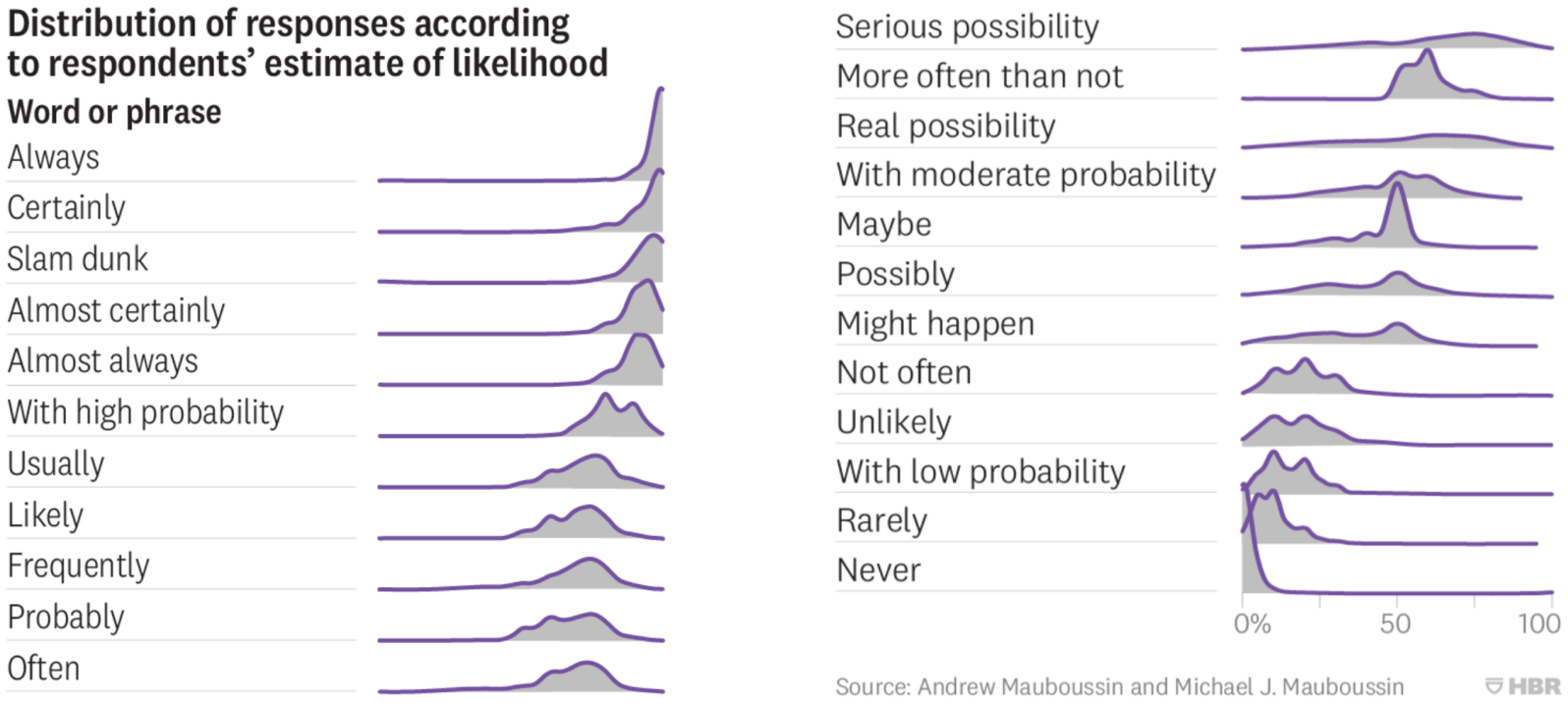
Verbal descriptions of probability and impact may not be interpreted equally

TABLE G-2: ASSESSMENT SCALE – LIKELIHOOD OF THREAT EVENT INITIATION (ADVERSARIAL)

Qualitative Values	Semi-Quantitative Values		Description
Very High	96-100	10	Adversary is **almost certain** to initiate the threat event.
High	80-95	8	Adversary is **highly likely** to initiate the threat event.
Moderate	21-79	5	Adversary is **somewhat likely** to initiate the treat event.
Low	5-20	2	Adversary is **unlikely** to initiate the threat event.
Very Low	0-4	0	Adversary is **highly unlikely** to initiate the threat event.

Source: NIST Special Publication 800-30 Rev1

SUBJECTIVITY



RISK QUANTIFICATION: UPGRADING TO FAIR

FAIR – FACTOR ANALYSIS OF INFORMATION RISK

- Leading quantification model for cyber risk – A standard taxonomy for information and operational risk
- Translates bits & bytes into dollars and cents
- An established and tested model (2001)
- Internationally accredited as an industry standard by The Open Group
- Adoption continues to permeate Fortune 100 (30%)
- Supported by a growing community of risk professionals
- Complementary analytical model to existing risk frameworks (ISO 31000, COSO, NIST CSF)

Tactical: Ability to provide discrete details on any given risk scenario

Strategic: Ability to examine risk in totality

A METHODOLOGY FOR QUANTIFYING AND MANAGING RISK IN FINANCIAL TERMS

This means it enables us to talk to the business in the language they speak best which is money.

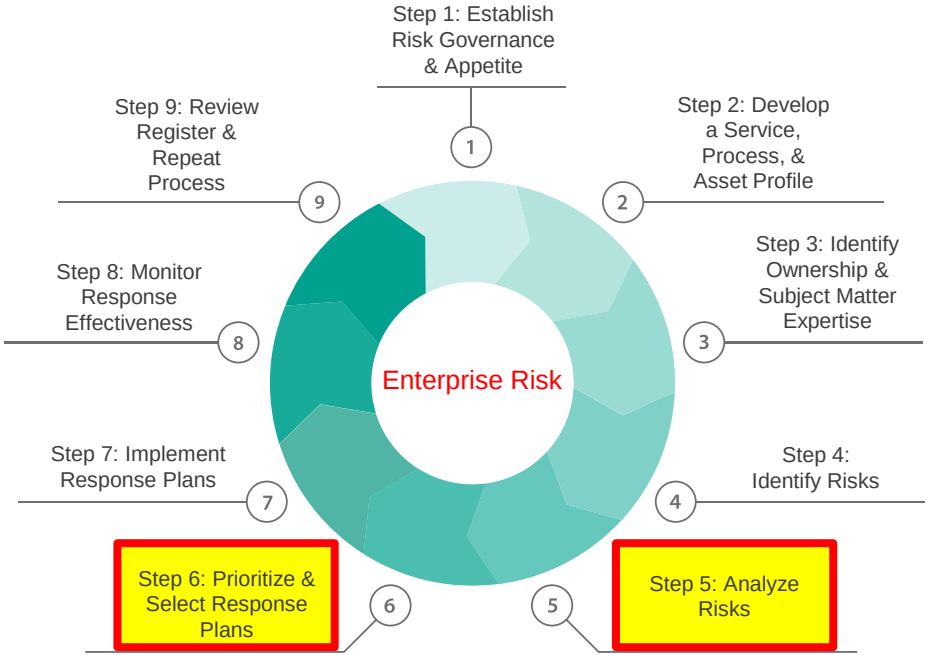
A COMPLEMENTARY ANALYTICS MODEL

- Complements Risk Frameworks, such as ISO 31000, COSO, NIST CSF, OCTAVE, …
- FAIR addresses activities such as **Risk Analysis, Risk Evaluation, Risk Treatment selection and prioritization** for which most standards do not provide pragmatic guidance.

- It is not a Risk Management Framework, but a well-reasoned and logical risk evaluation framework.
- It provides a scenario modeling construct to build and analyze risk scenarios.

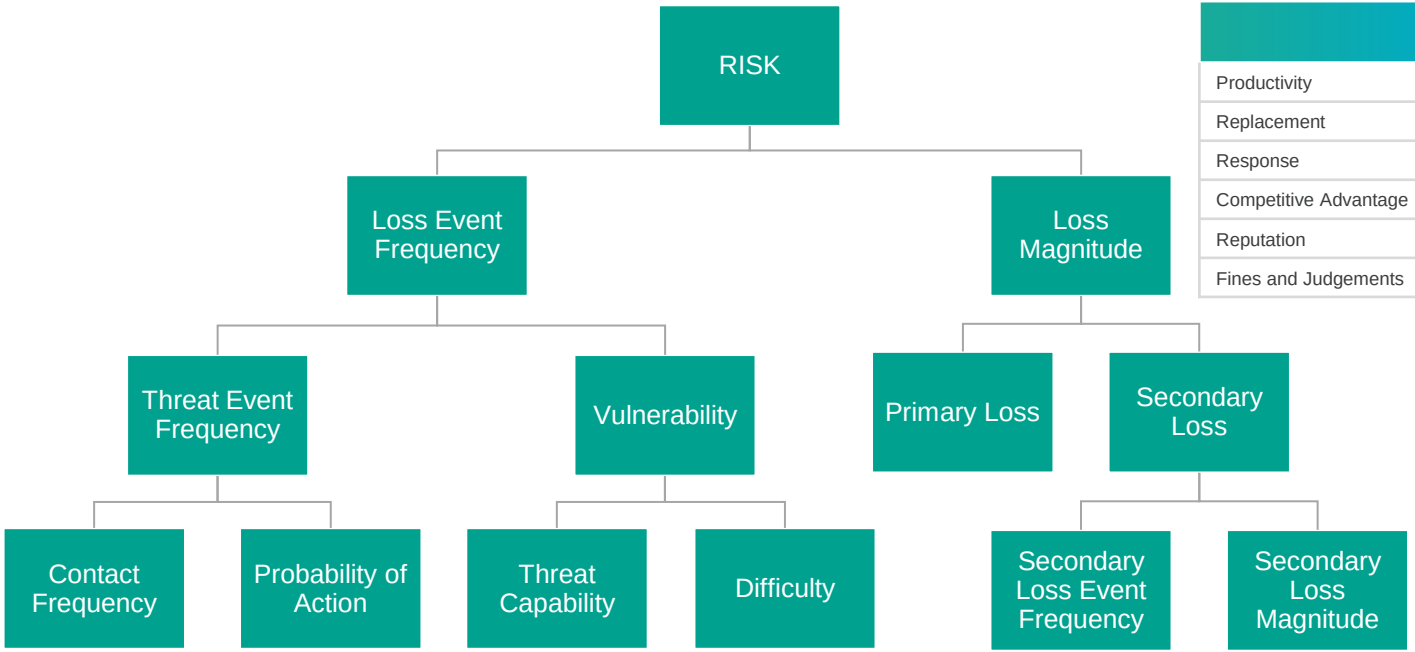
EXAMPLES OF WHERE FAIR FITS

ISO 31000



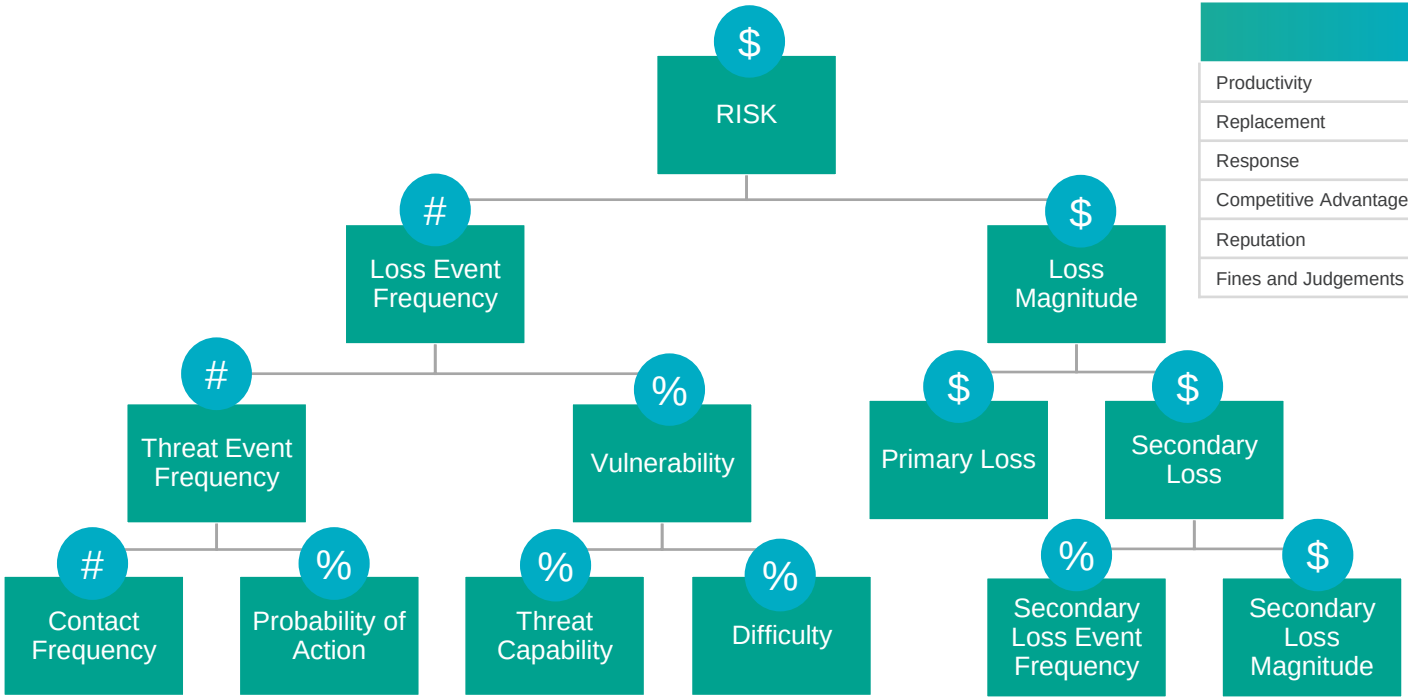
Octave

THE FAIR ONTOLOGY



	Primary Loss	Secondary Loss
Productivity	✓	
Replacement	✓	
Response	✓	✓
Competitive Advantage		✓
Reputation		✓
Fines and Judgements		✓

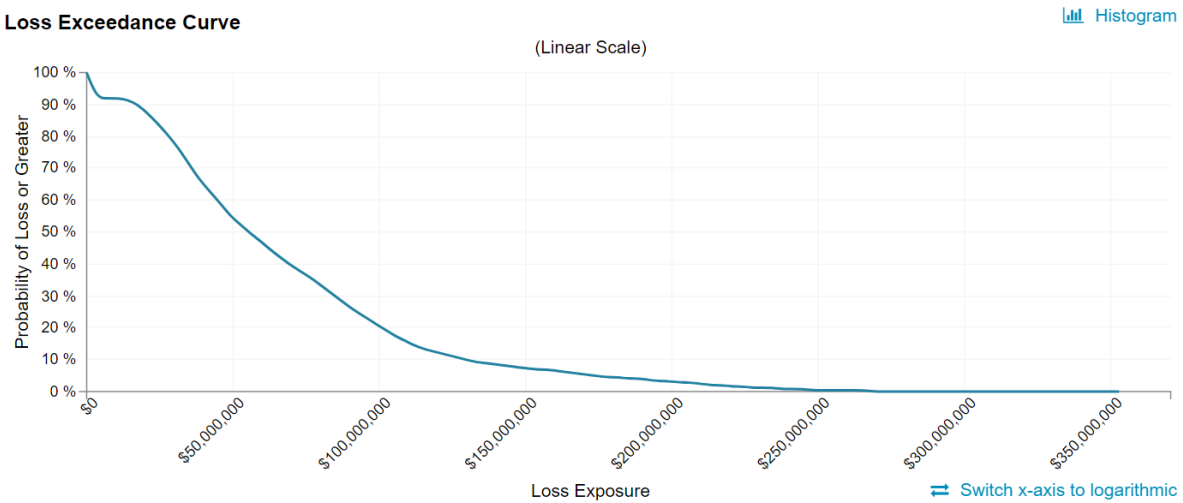
THE FAIR ONTOLOGY



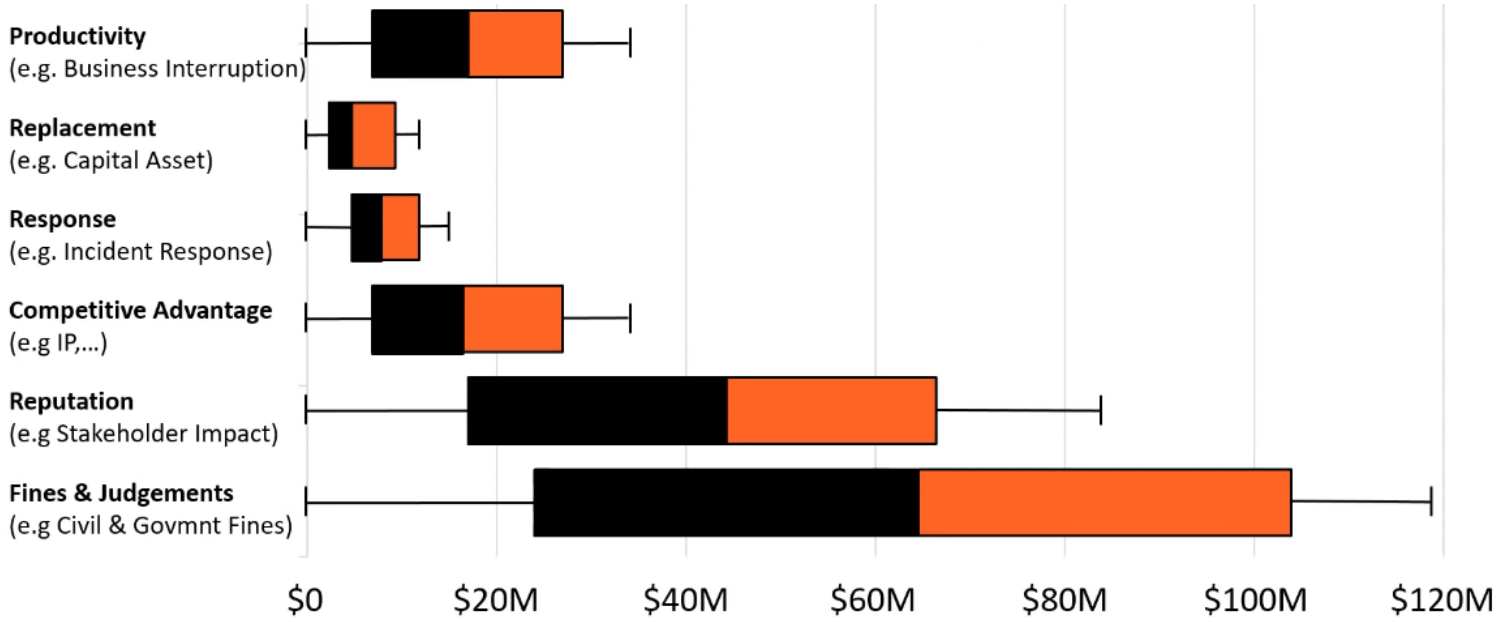
	Primary Loss	Secondary Loss
Productivity	✓	
Replacement	✓	
Response	✓	✓
Competitive Advantage		✓
Reputation		✓
Fines and Judgements		✓

WHAT ARE THE POSSIBLE OUTCOMES?

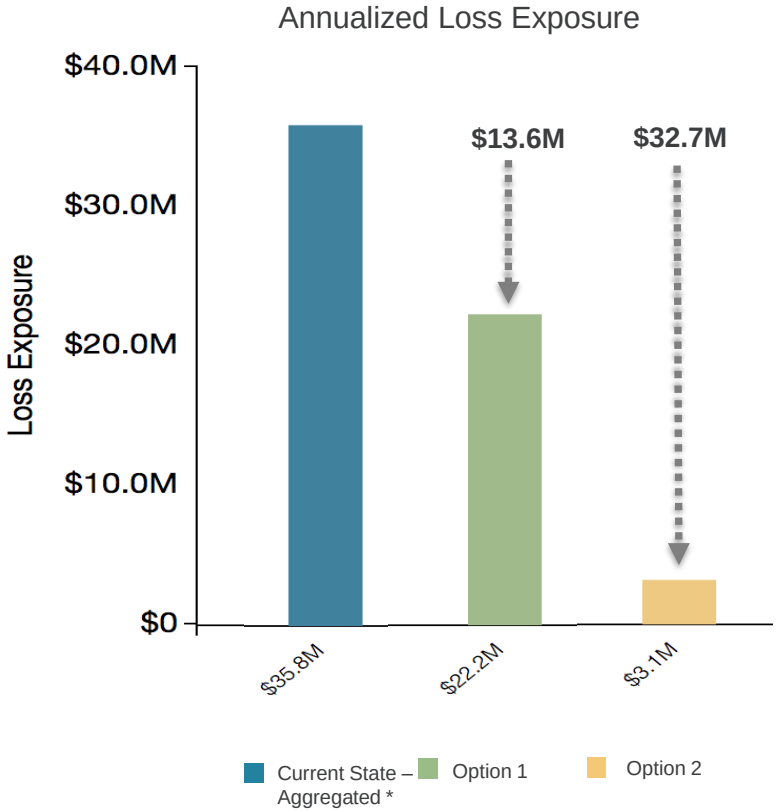
10th Percentile	Most Likely	90th Percentile
$17.1M	**$30.0M**	$129.6M
Min $0	Average $67.4M	Max $349.3M



UNDERSTAND WHAT'S AT RISK



TURN RISK DECISIONS INTO BUSINESS DECISIONS



Option 1	Option 2
$13.6M RISK REDUCTION	$32.7M RISK REDUCTION
VS.	VS.
$XX INVESTMENT	$XX INVESTMENT

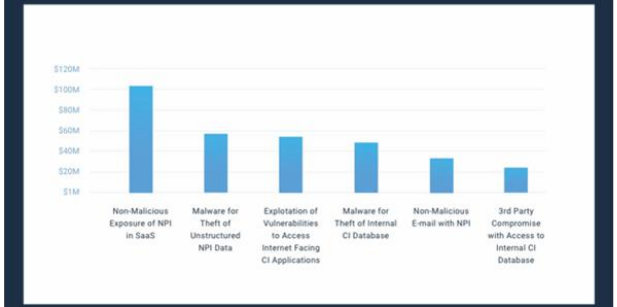
Action Items:

- **Pursue investment** based on ROI
- Revise **cyber insurance** policy
- **Accept risk** (no further action)

ANSWER BUSINESS QUESTIONS WITH DATA

HOW MUCH RISK DO WE HAVE?

WHAT ARE OUR TOP RISKS?



HOW IS RISK TRENDING VS APPETITE?

HAVE WE REDUCED RISK?

WHAT TYPES OF LOSS CAN WE EXPECT?

WHAT IS THE COST-BENEFIT OF THIS PROJECT?

CONCLUSION

CONCLUSION

CONNECT WITH THE SPEAKERS

Reach out to the speakers and learn more about their background

Kevin Strope
Protiviti
Director, Data Privacy
Kevin.Strope@protiviti.com
LinkedIn: https://www.linkedin.com/in/kevin-strope-899b925/

Matt Thomson
Protiviti
Associate Director, Security and Privacy
Matt.Thomson@protiviti.com
LinkedIn: https://www.linkedin.com/in/matt-thomson-infosec/

Face the Future with Confidence

protiviti®